UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

FILED
MAR 06 2015
IN THIS OFFICE
Clerk U. S. District Court
Greensboro, N.C.
By

United States of America
v.
LIN CHENG

Defendant(s)

Case No. 1:15MJ96-1

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of March 4, 2015 in the county of Orange in the Middle District of North Carolina, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. Section 1001(a)(2)	False Statements

This criminal complaint is based on these facts:

(See attached Affidavit of Special Agent Patrick S. Berckmiller)

☑ Continued on the attached sheet.

Patrick S. Berckmiller
Complainant's signature

Patrick S. Berckmiller, Special Agent - FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 3/6/2015

Joi Elizabeth Peake
Judge's signature

City and state: Winston-Salem, NC

Joi Elizabeth Peake, Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN THE MATTER OF A CRIMINAL COMPLAINT REGARDING LIN CHENG	Case No. 1:15MJ 96-1

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A COMPLAINT

1. I, Patrick S. Berckmiller, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

2. I am a Special Agent of the Federal Bureau of Investigation (FBI) and have been so employed since November, 1998. Since March, 1999, affiant has been assigned to investigate foreign counterintelligence and theft of trade secrets crimes. Affiant received training from the FBI regarding foreign counterintelligence and theft of trade secrets, and has previously been involved in investigations involving espionage, export violations, bank robbery, kidnapping, fugitives from justice, white collar crimes and computer crimes involving the theft of proprietary data. Most recently, I have been involved in an investigation regarding the theft of trade secrets. As a Federal Agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1001(a)(2) have been committed by Lin Cheng.

PROBABLE CAUSE

BACKGROUND OF LIN CHENG'S EMPLOYER

1. A United States based company [USC 1][1] maintains its global headquarters and information technology operations in Durham, North Carolina (NC). From November 17, 2008 until October 1, 2014, Lin Cheng had been employed at [USC 1] with her most recent position listed as a Scientist. Specifically, Lin Cheng was the engineering manager for [USC 1]'s fourth generation of [TECHNOLOGY 1].

2. On or about September 4, 2014, [USC 1] informed the Federal Bureau of Investigation that, on or about August 27, 2014, Lin Cheng emailed a file containing [USC 1]'s proprietary information from her work email at [USC 1] to email account

[1] In an effort to protect the identity of the victim company, its name has been withheld and is referred to as [USC 1].

nextgen0410@gmail.com. The file, titled [EXPORT FILE][2] contained [USC 1] trade secrets; specifically the step-by-step process [USC 1] uses to manufacture its [TECHNOLOGY 1].

3. According to Lin Cheng's immediate supervisor and other witnesses, [TECHNOLOGY 1] is the flagship product of a portion of [USC 1]'s business. Regarding the [EXPORT FILE] Lin Cheng sent from her work email to email account nextgen0410@gmail.com, Lin Cheng's supervisor and other [USC 1] employees estimated, that the information on [EXPORT FILE] would be worth in excess of $1 million. This transfer would allow the company to directly compete with [USC 1] in the current market. Additionally, [USC 1]'s supervisor and other [USC 1] employees determined that the proprietary and confidential files which were removed by Lin Cheng from the control of [USC 1] would cause both financial damage and technological loss to [USC 1].

LIN CHENG'S CONTACT WITH [SUBJECT 2][3]

4. The following information was discovered as a result of reviewing Lin Cheng's email account at [USC 1] and search warrant returns were issued on September 23, 2014 in the Middle District of North Carolina on Google. This warrant was for information pertaining to email account nextgen0410@gmail.com from the dates of January 1, 2013 to September 23, 2014. On or

[2] In an effort to protect the identity of the victim company, this file type is known within the company structure and is referred to as an [EXPORT FILE].

[3] In an effort to protect the identity of the victim company, the second subject's name has been withheld and is referred to as [SUBJECT 2].

about July 28, 2014, Lin Cheng received an email via LinkedIn from an individual who identified himself/herself as [SUBJECT 2], Chief Executive Officer (CEO) of Super Legend Holdings Limited. [SUBJECT 2]'s email to Lin Cheng included the following:

Dear Lin Cheng;

I am currently cooking a new venture of [TECHNOLOGY 1] / Process in China. The first phase is RMB 1 billion and goes to 2 billions for the 2nd phase. Please let me know if you are interested in this project.

5. On or about August 5, 2014, Lin Cheng used email account nextgen0410@gmail.com to send the following email to aresfang@foxmail.com:

Dear [SUBJECT 2],

This is Lin Cheng. Thank you for your kind email to me through LinkedIn. Can you please help me understand your proposal on the [TECHNOLOGY 1] Project in more details?

6. On or about August 5, 2014 through August 6, 2014, [SUBJECT 2] and Lin Cheng continued to exchange emails, which included the following excerpts:

Lin Cheng:

The project sounds interesting at this level. What would be your projected timeline and organization at this point?
[SUBJECT 2]:

It is planned that the project can be kicked off by the end of this year … it will be perfect if you are interested on it too.

Lin Cheng:

I am interested in any good [TECHNOLOGY 1] project. I would like to know what you are expecting from me and what kind of other expertise you have gathered so far.

[SUBJECT 2]:

I would like to invite you to join the project as the TD VP at the beginning of the project and move to RD VP for developing new devices once the production line starts…I would try to match the net income as you do in the US, stock option and other fringe benefits. Most of all it reveals the opportunity for you to contribute to your home country. There will be no ceiling effect in the home country. We all know this, right?

7. On or about August 11, 2014, [SUBJECT 2] and Lin Cheng continued to exchange emails, which included the following excerpts:

Lin Cheng:

Thanks for your invitation again. I am still checking with our legal person about a non-compete agreement that I have with my current employer. Therefore I can't make any commitment to you now. If you don't mind, can you please keep me updated with your project progress? I will let know when I hear back from our legal person.

[SUBJECT 2]:

Thanks for your honest. Of course, I never broke any law in any country. However, there are a few ways to avoid the infringement in a legal way. For instance, there is a common practice in the [TECHNOLOGY 1] industry now, that the designated person will be hired by a OBU paper company instead of a project company for a certain period of time until the bondage period is over. For your information, there is one of your current colleague is likely join the project . . . Of course, I would need to go over your CV before final decision. Can I have your correspondences of

WeChat and Mobile Phone for the cases of short and urgent communication?

8. On or about August 12, 2014, Lin Cheng told a [USC 1] executive that an individual named [SUBJECT 2] had contacted him/her via LinkedIn and offered him/her a job in the [TECHNOLOGY 1] field. Lin Cheng also used her work email account at [USC 1] to forward to the [USC 1] executive five emails dated August 5, 2014 through August 11, 2014. However, the emails Lin Cheng gave [USC 1] included references to topics not reflected in the emails Lin Cheng provided. The investigation determined that Lin Cheng edited the emails which were provided to [USC 1] and did not reflect all of the content of the communications between Lin Cheng and [SUBJECT 2]. An example of the differences between these emails is as follows: The investigation determined that Lin Cheng did not provide three of the eight email communications that had taken place between Lin Cheng and [SUBJECT 2], and of the five email communications Lin Cheng provided to [USC 1], four of the email communications had been edited and did not reflect all of the content of the communications between Lin Cheng and [SUBJECT 2]. For example, four lines of text (crossed out below) were removed from the communication Lin Cheng gave to [USC 1]:

Thanks for your honest. Of course, I never broke any law in any country. However, there are a few ways to avoid the infringement in a legal way. ~~For instance, there is a common practice in the [TECHNOLOGY 1] industry now, that~~

~~the designated person will be hired by a OBU paper company instead of a project company for a certain period of time until the bondage period is over.~~ For your information, there is one of your current colleague is ~~likely~~ join the project ~~too~~ . . . Of course, I would need to go over your CV before final decision. Can I have your correspondences of WeChat and Mobile Phone for the cases of short and urgent communication?

9. Additionally, [USC 1] determined that Lin Cheng never consulted with the [USC 1]'s legal department in regards to Lin Cheng's non-compete agreement at [USC 1].

10. On or about August 27, 2014 at 6:44 p.m., Lin Cheng emailed the [EXPORT FILE] which is a trade secret of [USC 1] from her work email account at [USC 1] to email account nextgen0410@gmail.com.

11. On or about September 13, 2014 at 8:02 p.m. nextgen0410@gmail.com received an email from aresfang@foxmail.com, subject "[TECHNOLOGY 1]." The email included the following:

Dear Lin Cheng;

The funding of the [TECHNOLOGY 1] project is much more smooth then it was expected . . . if you are not coming back to China or Shanghai in the near future, I need to have a conference call with you at your early convenience . . . it will be my great pleasure if you can join the project.

12. On September 20, 2014 at 7:22 p.m. nextgen0410@gmail.com received an email from aresfang@foxmail.com, subject "[TECHNOLOGY 1]". The email included the following:

Dear Lin Cheng;

I wonder if you did receive my e-mail sent to you on Sept. 14. The [TECHNOLOGY 1] Project in China is going much better than it was expected . . . Can you let me know your firm intention at this moment? We can work on the solution to project you from the legal infringement if you have firm intention.

LIN CHENG'S THEFT OF TRADE SECRETS FROM [USC 1]

13. [USC 1] reviewed logs of Lin Cheng's computer activity and discovered Lin Cheng had used her work laptop to download more than 16,000 files from [USC 1]'s servers. [USC 1] also discovered that, on or about August 27, 2014 at 6:44 p.m., Lin Cheng emailed the [EXPORT FILE] from her work email account at [USC 1] to email account nextgen0410@gmail.com.

LIN CHENG'S USE OF EMAIL ACCOUNT NEXTGEN0410@GMAIL.COM

14. A search warrant was issued on September 23, 2014 in the Middle District of North Carolina on Google. This warrant was for information pertaining to email account nextgen0410@gmail.com from the dates of January 1, 2013 to September 23, 2014. The following additional information was discovered as a result of the search warrant. Email account nextgen0410@gmail.com was created on or about April 24, 2013 at 4:57 p.m. The telephone number linked to the account is 919-599-5086, which I know from this investigation to be Lin Cheng's cellular telephone number. A review of email account nextgen0410@gmail.com revealed Lin Cheng used it: as a

repository for [USC 1] proprietary information forwarded from her work email account; to communicate with [SUBJECT 2]; and to communicate with a New York based book publisher. However, Lin Cheng's nextgen0410@gmail.com account was primarily used by Lin Cheng to communicate with [SUBJECT 3][4].

15. [SUBJECT 3] is a former [USC 1] employee who currently works for the UNITED STATES Government. There were only nine contacts listed in the address book of Lin Cheng's nextgen0410@gmail.com email account. These included three contacts affiliated with Lin Cheng's email addresses: salinda18@yahoo.com, work email account at [USC 1], and lcfjlinda@gmail.com. [USC 1] advised that salinda18@yahoo.com email account belongs to Lin Cheng. A review of Lin Cheng's email account at [USC 1] found an email sent to Lin Cheng on or about April 12, 2014 at 8:33 p.m. from yahoo-account-services-us@cc.yahoo.co-inc.com. The message advised Lin Cheng that **"Your Yahoo ID is: salinda18. The password for your Yahoo ID was recently changed."** A review of [USC 1]'s email account at [USC 1] determined that Lin Cheng used email account lcfjlinda@gmail.com to communicate with [USC 1] between the dates of October 8, 2014 and October 29, 2014. There was one unknown contact with email address infinity345@yahoo.com. There were two contacts affiliated with [SUBJECT 2]:

[4] In an effort to protect the identity of the victim company, the United States Government employee's name has been withheld and is referred to as [SUBJECT 3].

aresfang@foxmail.com and aresfang@gmail.com. There were three contacts affiliated with [SUBJECT 3]: [SUBJECT 3]@xx.xxx.gov, [SUBJECT 3]@xx.xxx.gov and 202779XXXX@vtext.com. The telephone number 202-779-XXXX, which I know from this investigation to be the cellular telephone number of the user of [SUBJECT 3].

16. On April 24, 2013 at 5:00 p.m., three minutes after creating the email account, Lin Cheng used nextgen0410@gmail.com to send an email to [SUBJECT 3]. The email stated:

> **Hi [SUBJECT 3],**
>
> **Hope all are excellent with you over DC. Just test if my personal email can get through your [xx.xxx.GOV] server. Thanks.**
>
> **[initials]**

17. On April 24, 2013 at 6:22 p.m. email account of [SUBJECT 3] responded to email account nextgen0410@gmail.com with the following:

> **Excellent. It came through just fine. Thank you. I like nextgen – creative!! briefing went really well. Now rushing to catch the train.**
>
> **[SUBJECT 3]**

18. As mentioned above, Lin Cheng used the nextgen0410@gmail.com account as a repository for [USC 1] proprietary information she forwarded, without authorization, from her work email account. Many of the emails sent from [USC 1]'s work email account to the nextgen0410@gmail.com email account, including the August 27, 2014 email with the [EXPORT

FILE], included the following [USC 1] proprietary warning reminder in the body of the email:

> **This e-mail message, including any attachments and previous email messages sent with it, contains CONFIDENTIAL and PROPRIETARY information of [USC 1] or its subsidiaries and may be legally PRIVILEGED. You may not use, disclose, reproduce or distribute such information without [USC 1]'s authorization. If you have received this message in error, please notify the sender immediately and permanently delete the original message, its attachments, and any copies thereof.**

19. Lin Cheng sent [USC 1] proprietary information from her work email account at [USC 1] to the nextgen0410@gmail.com email account on the following dates and times:

April 1, 2014	1:03 p.m.
April 26, 2014	1:35 p.m.
April 28 2014	8:49 p.m.
May 26, 2014	6:46 p.m.
August 3, 2014	4:39 p.m.
August 3, 2014	4:40 p.m.
August 27, 2014	6:44 p.m.

20. Lin Cheng also used the nextgen@0410@gmail.com account to send proprietary [USC 1] information to [SUBJECT 3]'s email account [SUBJECT 3]@xx.xxx.gov.

21. On or about May 14, 2013 at 8:43 a.m., Lin Cheng's work email account at [USC 1] sent an email to nextgen0410@gmail.com. On or about May 14, 2013 at 8:56 a.m.,

Lin Cheng used the nextgen0410@gmail.com email account to remove the [USC 1] proprietary information warning and one of the two attachments, and forwarded the email to [SUBJECT 3]@xx.xxx.gov. Each page of the 38-page attachment was marked "Confidential." On or about May 14, 2013 at 11:36 a.m. [SUBJECT 3]@xx.xxx.gov responded to the email from nextgen0410@gmail.com with **"Thanks much."**

22. Lin Cheng sent additional [USC 1] proprietary information to [SUBJECT 3]@xx.xxx.gov on the following date and time:

September 11, 2013 11:38 a.m.

23. According to [USC 1], Lin Cheng was not authorized to send proprietary [USC 1] information to the user of [SUBJECT3]@xx.xxx.gov and the user of [SUBJECT 3]@xx.xxx.gov was not authorized to receive proprietary [USC 1] information.

LIN CHENG'S ACKNOWLEDGEMENT OF PROTECTING TRADE SECRETS AND PROPRIETARY INFORMATION OWNED BY [USC 1]

24. On November 17, 2008, Lin Cheng signed the [USC 1] "Employee Agreement Regarding Confidential Information, Intellectual Property and Noncompetition," which states:

> **I understand that during my employment I may have access to nonpublic or otherwise confidential information relating to the Company…Such information, whether of a technical or non-technical nature, is referred to below as "Confidential Information."**
>
> **. . . On termination of my employment with the Company for any reason, I will promptly deliver to the Company all**

Company documents, records, files, notebooks, manuals, letters, notes, reports, customer and supplier lists, cost and profit data, apparatus, drawings, blueprints, and any other material of the Company, including all materials pertaining to Confidential information . . .

25. On August 13, 2013, Lin Cheng also signed a certification that she had reviewed the current [USC 1] Code of Conduct located on [USC 1]'s computer network. [USC 1]'s signature also certified to the statement "I understand that the Code of Conduct applies to me as an employee and I will conduct myself in accordance with the Code."

26. On November 14, 2014, a [USC 1] manager advised that she oversaw the implementation of [USC 1]'s High Security Environment (HSE). The HSE was designed as a repository for the most valuable files owned by [USC 1] which included [EXPORT FILES]. The HSE allows access to files, but in a read only format. The HSE was designed to be fully implemented on or about September 17, 2014. The additional protection given to access the HSE included a second RSA key token for remote access after initial logon is successful to the [USC 1] network with the first RSA key token. Prior to the implementation of the HSE [USC 1] also had badge access restrictions in place to control physical access of employees at building entrances and within buildings to various areas. Additionally, the network of [USC 1] has restrictions based on the employee's role at [USC 1]. Not every employee had access to all parts of the [USC 1]

network. Further, the protections were in place to prevent public access to proprietary files and [TECHNOLOGY 1]. On or about April 11, 2014, this [USC 1] manager had an in-person meeting with Lin Cheng and discussed the protection of [EXPORT FILES] as they were scheduled to be moved into the HSE. The HSE was implemented in phases and this meeting discussed this particular phase. Lin Cheng expressed an understanding as to why the [EXPORT FILES] needed to be moved into the HSE. On or about June 17, 2014, this [USC 1] manager sent an email to Lin Cheng including instructions to move [EXPORT FILES] in order to facilitate the transition to the HSE which restricted access even further to the most valuable data which [USC 1] sought to protect. It was determined that Lin Cheng failed to move 14 such files as requested.

After the implementation of placing the [EXPORT FILES] into the HSE, this same [USC 1] manager sat down personally with Lin Cheng after Lin Cheng returned from travel to make sure the HSE was properly working for Lin Cheng to do her job. This [USC 1] manager recalled that the logon process worked on the first attempt with Lin Cheng. This [USC 1] manager reviewed [USC 1] computer logs and determined that Lin Cheng accessed the HSE on six occasions between August 19, 2014 and September 9, 2014. On or about September 17, 2014, the [USC 1] network was scanned again and all remaining [EXPORT FILES] on the network were found and moved.

LIN CHENG'S SUSPENSION AND TERMINATION FROM [USC 1]

27. On or about September 12, 2014, Lin Cheng was suspended from [USC 1]. [USC 1] took possession of Lin Cheng's badge access card to [USC 1] facilities, laptop computer, remote access RSA key tokens and [USC 1] credit card.

28. On or about September 12, 2014, Lin Cheng used nextgen0410@gmail.com to inform the user of [SUBJECT 3]@xx.xxx.gov via email that she had been suspended from [USC 1]. The subject line of the first email was "URGENT!!!" The following are excerpts from the emails exchanged that day:

Lin Cheng:

Have to cancel the ECCE trip. I am in a big trouble. Can you call me when you can?

[SUBJECT 3]@xx.xxx.gov:

I cant call but tell me briefly what the problem is?

Lin Cheng:

Can I text you?

[SUBJECT 3]@xx.xxx.gov:

I am home...Just write something short.

[SUBJECT 3]@xx.xxx.gov:

Just send me a short email. Be vague.

Lin Cheng:

I may need your help to find a job in a few weeks or so. I am currently suspended with a shock. The IS complained that I have too many files saved on my laptop. I explained that I copied them for myself to work at home and during a travel. They said that was against company's policy and they need to check all the files. If everything is okay, I can go back to work. But now, I can't access to any company's facility. [initials] took all my identities. I told that I never did anything against the company. I am very very sad about this.

[SUBJECT 3]@xx.xxx.gov:

Don't worry!! [USC 1] is like this. Hope they don't track anything that u sent to me!!

Lin Cheng:

Shouldn't. We didn't say bad thing but exchange mostly technical opinions as professionals. So don't worry. I guess that They probably "worry" if I sent anything to China, which I never ever did anything.

[SUBJECT 3]@xx.xxx.gov:

They will check ur emails

Lin Cheng:

But not personal emails, right?

[SUBJECT 3]@xx.xxx.gov:

They can't unless u give them ur gmail password.

29. That same day, on or about September 12, 2014 at 8:01 p.m. nextgen0410@gmail.com received a notification from Google that the account's password had recently been changed.

30. Later that same day, or about September 12, 2014 at 8:48 p.m., Lin Cheng used the nextgen0410@gmail.com email

account to forward the [USC 1] [EXPORT FILE] to email account salinda18@yahoo.com, which I know from this investigation to be another email account used by Lin Cheng. The email forwarded from nextgen0410@gmail.com to salinda18@yahoo.com still had the [USC 1] proprietary warning reminder, as previously detailed above. A review of USB electronic storage media returned to [USC 1] by Lin Cheng also found an additional 74 [EXPORT FILES] which are trade secrets owned by [USC 1].

31. On or about September 17, 2014, Lin Cheng was asked by [USC1] company officials to return any USB drives that Lin Cheng had plugged into [USC1] computers. On September 17, 2014, Lin Cheng arrived at [USC 1] and returned six USB drives from Lin Cheng's home or another location outside of [USC 1] controlled space. Lin Cheng texted a [USC 1] employee and indicated, "**…I am taking all the USB drives that I can find at home to Building 16 now. Will take me about 20mins to get there. Will you be there then…**" A forensic review confirmed that all six of these USB drives were connected to Lin Cheng's assigned laptop computer owned by [USC1].

32. On September 18, 2014, a [USC1] executive had further communication with Lin Cheng via text messaging, requesting Lin Cheng to return a SanDisk Cruzer USB drive which was identified as being connected to Lin Cheng's issued Dell E6230 laptop computer in the August/September 2014 timeframe.

33. On or about September 22, 2014, Lin Cheng returned an additional USB drive to [USC 1], identified as a SanDisk Cruzer Blade. A forensic review determined that this USB drive was not connected to either of Lin Cheng's assigned [USC1] computers.

34. On or about October 1, 2014, [USC 1] terminated Lin Cheng's employment based on her having transferred confidential and proprietary information belonging to the company to devices owned or controlled by Lin Cheng and not accessible by [USC 1] and for engaging in other violations of company policies and procedures related to [USC 1]'s proprietary information and trade secrets. Lin Cheng was asked by [USC 1] company officials to return four specific USB drives, including one USB drive which was plugged into an Apple product. Lin Cheng stated that she did not own an Apple computer, but her spouse may have two USB drives and may have used them for a church sermon. Lin Cheng was provided a letter in person on October 1, 2014. The content of this letter is as follows:

> **Dear Lin Cheng:**
>
> **[USC 1] has learned that you have transferred confidential and proprietary information belonging to the company to devices owned or controlled by you and not accessible by [USC 1] and have engaged in other violations of company policies and procedures relating to [USC 1]'s proprietary information and trade secrets. [USC 1] hereby demands that you immediately turn over to [USC 1] any and all storage or other devices onto which you have transferred [USC 1]'s property, return to [USC 1] any documents or other property in your possession and provide [USC 1] with all information**

needed to access any account, service or other location where you have stored company assets.

If you do not immediately comply with [USC 1]'s demands by returning and/or providing [USC 1] access to and control of [USC 1] property you have misappropriated, the company intends to pursue all available civil and legal remedies and recourse against you.

35. As a result of a search warrant to Google, Incorporated, it was learned that later that same day, on October 1, 2014 at 2:13 p.m., the email account nextgen0410@gmail.com was deleted.

36. After being terminated from employment at [USC 1], Lin Cheng utilized email and text messages to communicate. On or about October 7, 2014, Lin Cheng communicated with an executive employee of [USC 1] via text messages. The screenshots of these text messages were affiliated with email account lcfjlinda@gmail.com. Lin Cheng also utilized the email account lcfjlinda@gmail.com between October 8, 2014 and October 29, 2014 in order to communicate with [USC 1].

37. On or about October 8, 2014, [USC 1]'s executives learned that, on or about June 10, 2014, Lin Cheng, without [USC 1]'s authorization, had signed a contract with Nova Publishing to write a book on the topic of Lin Cheng's area of expertise. Due to the nature of the topic having been gained with additional experience from [USC 1], the book would not have been

approved if Lin Cheng had sought the required authorization from [USC 1].

LIN CHENG'S INSTRUCTIONS TO [SUBJECT 3] TO DELETE EMAILS

38. On or about July 3, 2013, Lin Cheng sent a message to the user of [SUBJECT 3]@xx.xxx.gov:

Sorry ... Please also empty your trash folder.

Additionally, on or about January 6, 2014, Lin Cheng sent a message to the user of [SUBJECT 3]@xx.xxx.gov:

> **Okay. Still a little bit.. will talk at 4pm. Already deleted all the emails.**

LIN CHENG'S USE OF FLASH MEDIA AND EXTERNAL STORAGE DEVICES

39. On or about August 7, 2013 a new laptop computer was issued by [USC 1] to Lin Cheng. This computer was identified by [USC 1] as a Dell Latitude E6230 with an affixed [USC 1] barcode 056CPU.

40. On or about November 10, 2013, Lin Cheng requested an encrypted USB drive. The standard issue from [USC 1] is a Kingston Data Traveler which would have been issued within a few days of Lin Cheng's request. This is the only authorized USB drive at [USC 1] and is owned by [USC 1].

41. On or about September 12, 2014, Lin Cheng was suspended from [USC 1] with no access to company facilities. [USC1] retained Lin Cheng's Dell Latitude E6230 laptop computer,

leaving Lin Cheng with no access to electronic devices owned by [USC 1] in order to communicate.

42. A white Verbatim brand 4GB flash USB drive labeled "IPEC" that was provided by Lin Cheng to [USC1] on September 17, 2014 was forensically reviewed on November 19, 2014. This device contained two hidden directories named ".trashes" and ".spotlight." Based on my training and experience, the presence of these hidden directories indicates that the device had been plugged into a computer running an Operating System created by Apple, Inc.[5]

43. The forensic review also determined that the following items were connected to Lin Cheng's laptop computer owned by [USC 1]. These items are unaccounted for and are not in the possession of [USC 1] or the FBI: USB flash drives, cellular telephones, and external portable hard drives.

44. A forensic review identified approximately 50 unique USB devices having been connected to either the [USC 1] desktop computer, the [USC 1] laptop, or both. The FBI has identified six of the 50 evidence items in their possession. Of the remaining 44, approximately 28 USB devices were found to be

---

[5] A hidden directory is a directory that is not normally visible when examining the contents of the directory in which is resides.

affiliated with the laptop, approximately 20 USB devices were found to be affiliated with the desktop computer, and four were identified as having been connected to both machines.

45. The forensic review also identified 130 files on flash media provided by Lin Cheng to [USC 1] which were marked as confidential or proprietary and are the property of [USC 1]. An additional 74 files were confirmed as [EXPORT FILES] and contain recipe information for [USC 1] products. [USC 1] identified these files as trade secrets and are the property of [USC 1].

46. As of February 23, 2015, Lin Cheng has not returned to [USC 1] any additional property or files that have been taken from [USC 1].

47. The investigation determined that Lin Cheng departed the United States on December 27, 2014 with a destination of Beijing Capital International Airport, The People's Republic of China. Lin Cheng arrived back in the United States on January 8, 2015 from Pu Dong, Shanghai, The People's Republic of China.

48. On or about February 19, 2015, the email address salinda18@yahoo.com was reviewed pursuant to a search warrant returned with negative results for the previously identified forwarded email from nextgen0410@gmail.com of the [TECHNOLOGY 1] files. Based upon training and experience, the email was deleted, forwarded to another email address, or transferred to an electronic storage media and then deleted.

49. As a result of the investigation, a criminal search warrant was executed on March 4, 2015 at Lin Cheng's residence of 103 S. Crabtree Knolls, Chapel Hill, North Carolina 27514. Cheng agreed to a voluntary interview with FBI Special Agent Patrick Berckmiller and Department of Energy Special Agent Kevin Gordon. Cheng agreed to have the interview recorded with an audio device. Cheng was advised of the identity of the interviewing agents. Cheng was also advised that she needed to be truthful during the interview and could be prosecuted if she provided false information. Cheng acknowledged an understanding to this statement.

FALSE STATEMENT ONE

50. During the interview, Cheng was specifically asked **"Do you have any information that still belongs to [USC 1]?"** Cheng responded **"Hmmm, well published paper as I said. I keep some copies and pretty much that and some meeting slides you know."** During the course of the search, a box with the word "[USC 1]" in blue letters was found in plain view in Cheng's bedroom next to her packed luggage. Cheng also disclosed during the interview that she was scheduled to depart to Purdue University on a flight at about 9:40am. Upon opening the box, there were two sealed bags also identified with [USC 1] markings which contained a total of 11 parts. On March 4, 2015, Special Agent Patrick Berckmiller and Special Agent Kevin Gordon took

this box of 11 parts and showed them to [USC 1] Company officials. These officials determined that these items are the property of [USC 1] or clients of [USC 1] and were valued in excess of several thousands of dollars. Further these parts should not be located within the residence of Lin Cheng.

51. On March 4, 2015, a computer preview was conducted of Lin Cheng's Toshiba laptop during the search of Cheng's residence. During this preview, it was determined that the computer's hard drive contained the [EXPORT FILE] which has previously been identified as a trade secret.

FALSE STATEMENT TWO

52. During the interview of Lin Cheng on March 4, 2015, she was asked regarding her communication with [SUBJECT 2], "And you reported again all that information to [USC 1 Executive]? Cheng responded "**To** [USC 1 Executive], **to** [USC 1 Executive]". Question: "So he knew everything?" **Cheng: "yeah"** Question: "that was going on between you and [SUBJECT 2] is that correct?" **Cheng: "Right, right, right"** Question: "all the communications? **Cheng: "Right, right, right, right."**

53. [USC 1 Executive] confirmed that he was not provided all or complete communications between Cheng and [SUBJECT 2].

FALSE STATEMENT THREE

54. During the interview of Cheng on March 4, 2015, Cheng stated **"I did everything for the work and I wouldn't never ever transfer or tell any information to the external people outside of [USC 1]."**

55. Based on the forgoing, I request that the Court issue the proposed arrest warrant.

Respectfully submitted,

Patrick S. Berckmiller
Special Agent
Federal Bureau of
Investigation

Subscribed and sworn to before me on
3/6, 2015

JOI ELIZABETH PEAKE
UNITED STATES MAGISTRATE JUDGE
MIDDLE DISTRICT OF NORTH CAROLINA